

550, 011

Rec'd PCT/PTO 19 SEP 2005

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international(43) Date de la publication internationale
14 octobre 2004 (14.10.2004)

PCT

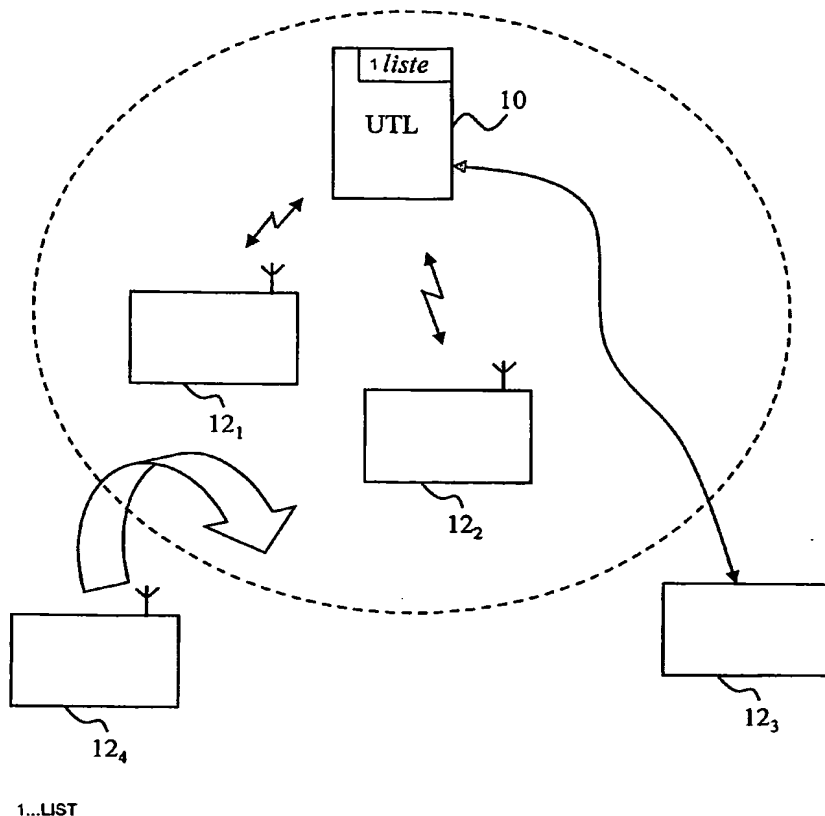
(10) Numéro de publication internationale
WO 2004/088569 A2

- (51) Classification internationale des brevets⁷ : **G06K**
- (21) Numéro de la demande internationale : **PCT/FR2004/000556**
- (22) Date de dépôt international : 9 mars 2004 (09.03.2004)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
03/03241 17 mars 2003 (17.03.2003) FR
- (71) Déposant (pour tous les États désignés sauf US) :
OBERTHUR CARD SYSTEMS S.A. [FR/FR]; 102,
boulevard Malesherbes, F-75017 Paris (FR).
- (72) Inventeur; et
- (75) Inventeur/Déposant (pour US seulement) : **DU-MORTIER, Gilles** [FR/FR]; 7, rue de l'Amiral, F-95000 Cergy (FR).
- (74) Mandataire : **SANTARELLI**; 14, Avenue de la Grande Armée, B.P. 237, F-75822 Paris Cedex 17 (FR).
- (81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,

[Suite sur la page suivante]

(54) Title: METHOD OF COMMUNICATING BETWEEN DIFFERENT ELECTRONIC ENTITIES

(54) Titre : PROCEDE DE COMMUNICATION ENTRE DIVERSES ENTITES ELECTRONIQUES



(57) Abstract: The invention relates to a method of communicating between at least two electronic entities (12₁, 12₂, 12₃), involving a communication management unit (10) which uses a command/response protocol in order to communicate with the electronic entities (12₁, 12₂, 12₃). According to the invention, at least one of the aforementioned electronic entities (12₁, 12₂) communicates with the communication management unit (10) using wireless technology. The inventive communication method comprises a step consisting in saving a list of electronic entities in the communication management unit (10). The invention can be used for microcircuit cards.

(57) Abrégé : Ce procédé de communication entre au moins deux entités électroniques (12₁, 12₂, 12₃) fait intervenir une unité (10) de gestion des communications qui utilise un protocole commande-réponse pour communiquer avec les entités électroniques (12₁, 12₂, 12₃). Au moins une des entités électroniques (12₁, 12₂) communique avec l'unité (10) de gestion des communications en

[Suite sur la page suivante]

WO 2004/088569 A2



PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

- (84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE DE COMMUNICATION ENTRE DIVERSES ENTITES ELECTRONIQUES

L'invention se rapporte à un procédé de communication entre diverses entités électroniques.

Elle s'applique à des systèmes de communication qui mettent en œuvre un protocole de communication du type commande-réponse. Dans ce type de systèmes, une unité de gestion des communications commande au moins en partie le déroulement des communications entre un ensemble d'entités électroniques en envoyant des commandes à chacune des entités électroniques de cet ensemble, qui, après traitement de ces commandes – lesquelles impliquent éventuellement des calculs complexes – se contentent de répondre aux commandes reçues.

L'unité de gestion des communications peut être par exemple un terminal, qui fait éventuellement partie de l'ensemble des entités électroniques communicantes. C'est le cas, par exemple, des cartes bancaires et des terminaux de paiement actuels. Le terminal exécute un programme de commande du déroulement des communications entre lui-même et la carte bancaire à microcircuit.

On estime qu'un besoin d'applications faisant communiquer entre elles plusieurs entités électroniques, notamment des entités sécurisées et portables, va apparaître d'ici deux à trois ans. Dès lors, des mécanismes de communication robustes et dynamiques seront nécessaires. Par exemple, des entités électroniques peuvent fréquemment et sans préavis se trouver temporairement hors de portée de communication. Un problème de perte potentielle de messages en cours de diffusion peut alors survenir.

La présente invention a pour but de remédier à cet inconvénient.

Dans ce but, l'invention propose un procédé de communication entre au moins deux entités électroniques, ce procédé faisant intervenir une unité de gestion des communications qui utilise un protocole commande-réponse pour communiquer avec les entités électroniques, ce procédé étant remarquable en ce qu'au moins une des entités électroniques communique avec l'unité de gestion des communications en utilisant une technologie sans fil, et en ce qu'il

comporte une étape consistant à mémoriser dans l'unité de gestion des communications une liste desdites entités électroniques.

Ce procédé, particulièrement bien adapté à un protocole commande-réponse, autorise ainsi une présence intermittente d'une ou plusieurs entités électroniques dans le rayon d'action de l'unité de gestion des communications sans perte de messages en cours de diffusion, sachant que seuls les messages à émettre ou à recevoir par les entités électroniques contenues dans la liste mémorisée dans l'unité de gestion des communications seront traités. Par "rayon d'action", on entend la région au sein de laquelle la communication est possible entre l'unité de gestion des communications et les entités électroniques. A titre d'exemple nullement limitatif, ce peut être un champ radiofréquence. Par extension, le rayon d'action inclut aussi les connexions de type filaire entre l'unité de gestion des communications et certaines entités électroniques.

On appelle UTL (Unité de Traitement Logique) l'unité de gestion des communications dans le cadre de l'application de l'invention à des cartes à microcircuit utilisant une technologie sans contact pour communiquer. De telles entités électroniques sont particulièrement bien adaptées à l'invention. Dans cette application, une UTL assure la communication avec des cartes à microcircuit sans contact lorsque celles-ci se trouvent dans son champ radiofréquence. L'UTL est en effet pourvue d'un lecteur sans contact de structure connue en soi, utilisé de façon non conventionnelle, dans un environnement à plusieurs microcircuits. Elle est utilisée de façon non conventionnelle au sens où c'est pour faire communiquer entre elles les différentes entités électroniques qu'on les place simultanément dans le champ de l'UTL, contrairement à une utilisation classique, où, lorsque plusieurs microcircuits se trouvent dans le champ de l'UTL, on en sélectionne un seul pour communiquer avec l'UTL. L'UTL peut être un simple ordinateur personnel (PC) classique.

Les entités électroniques d'un ensemble E commandé par l'UTL communiquent avec celle-ci par fréquence radio en utilisant un mécanisme de couplage capacitif ou inductif du type décrit dans les normes ISO/IEC 14443, 15693 ou 18000. La norme 14443 s'applique aux cartes d'identification dites de proximité (10 cm environ): "*Identification Cards – Contactless integrated circuit(s) cards – Proximity cards*". La norme 15693 s'applique aux cartes

d'identification dites de voisinage (70 cm environ): "*Identification Cards – Contactless integrated circuit(s) cards – Vicinity cards*". La norme 18000 en projet s'applique aux tags d'identification en communication radiofréquence et s'applique à différentes fréquences (125 kHz, 13,56 MHz, 443 MHz, 900 MHz, etc.).

Les applications utilisant les fréquences radio (WiFi, BlueTooth, etc.) ne sont pas a priori visées par l'invention. Néanmoins, l'invention pourrait s'appliquer dès lors qu'on se trouverait dans un schéma de communication du type commande-réponse avec une unité de gestion des communications. L'invention peut également s'appliquer aux communications avec contact, en utilisant par exemple une carte à microcircuit selon la norme ISO-7816.

Généralement, mais non nécessairement, l'UTL fournit l'énergie aux entités communicantes.

Selon une caractéristique particulière, les entités électroniques forment un réseau d'acointances, c'est-à-dire une liste des entités présentes dans le rayon d'action de l'unité de gestion des communications et susceptibles de communiquer entre elles.

Ce réseau d'acointances a pour avantage de présenter un caractère dynamique. Lors du démarrage du système, il peut être, soit vide, soit préprogrammé pour contenir une ou plusieurs entités électroniques.

Selon une caractéristique particulière, le procédé comporte une étape consistant, lorsque la liste d'entités mémorisée dans l'unité de gestion des communications comporte une nouvelle entité électronique, à ajouter la nouvelle entité électronique au réseau d'acointances en fonction d'au moins un critère prédéterminé.

Ainsi, lorsqu'une nouvelle entité électronique E entre en communication avec l'unité de gestion des communications, soit en s'y connectant physiquement, soit en entrant dans son rayon d'action, cette entité E est ajoutée au réseau d'acointances et y est enregistrée comme acointance d'une entité P déjà présente dans le réseau si et seulement si P et E sont amenées à communiquer entre elles par la suite. Un critère C peut être utilisé pour déterminer cette acointance. La nature de l'entité peut constituer un tel critère C. Le critère C dépend principalement de l'application. Le réseau d'acointances

peut ne contenir que deux entités, ou être réduit à une simple liste lorsque toutes les entités qui se trouvent dans le rayon d'action de l'unité de gestion des communications peuvent communiquer entre elles.

5 Selon une caractéristique particulière, le procédé de communication conforme à l'invention comporte une étape consistant à mémoriser un message destiné à au moins une des au moins deux entités électroniques précitées lorsque l'entité électronique destinataire est temporairement hors de portée de l'unité de gestion des communications.

10 Cela permet d'éviter de perdre des messages lorsqu'une entité sort temporairement du rayon d'action de l'unité de gestion des communications. Comme indiqué ci-dessus, la présence intermittente d'une entité électronique dans le rayon d'action de l'unité de gestion des communications est ainsi possible.

15 Selon une caractéristique particulière, à chacune des au moins deux entités électroniques précitées est associé un identifiant unique.

Cela constitue un moyen simple de désigner et d'identifier chaque entité électronique. Dans le cas où les entités électroniques sont des cartes à microcircuit, la norme 7816-6/AM1 spécifie un identifiant de fabricant ainsi que la construction d'un identifiant unique pour chaque microcircuit.

20 Selon une caractéristique particulière, à chaque identifiant est associé un code de service ou de famille d'applications (telle que définie dans la norme ISO 14443).

Cela permet de classer les entités électroniques selon leur nature et leur application et de préciser ainsi leur désignation et leur identification.

25 Selon une caractéristique particulière, le procédé de communication comporte une étape consistant à créer une boîte aux lettres dans l'unité de gestion des communications lorsque la liste d'entités qui y est mémorisée comporte une nouvelle entité électronique, cette boîte aux lettres étant adaptée à recevoir et mémoriser des messages destinés à ou envoyés par la nouvelle
30 entité électronique.

Les messages en attente de traitement sont ainsi sauvegardés dans cette boîte aux lettres.

Dans un mode particulier de réalisation, le procédé comporte des étapes suivant lesquelles l'unité de gestion des communications :

- parcourt la liste des entités électroniques,
- demande à chaque entité électronique si elle a un message à envoyer et, si c'est le cas,
- mémorise ce message dans une boîte aux lettres,
- envoie le message à l'entité électronique destinataire du message lorsqu'elle est joignable, puis
- supprime le message de la boîte aux lettres.

10 Ainsi, la liste et la boîte aux lettres permettent une gestion simple à mettre en œuvre et efficace des messages par l'unité de gestion des communications.

Cette boîte aux lettres est par exemple une boîte de réception, c'est-à-dire qu'elle contient les messages en attente à destination de l'entité à laquelle elle est associée.

15 Cela constitue le cas le plus courant.

Dans un mode particulier de réalisation, le procédé de communication fait intervenir au moins trois entités électroniques et l'unité de gestion des communications se confond avec une des entités électroniques.

20 Ainsi, l'unité de gestion des communications est dite participante : elle participe aux échanges de messages avec les autres entités électroniques.

Selon une caractéristique particulière, l'unité de gestion des communications sert de proxy, c'est-à-dire d'intermédiaire, pour accéder à au moins une des entités électroniques.

25 Cette fonction supplémentaire conférée à l'unité de gestion des communications est pratique et simple à mettre en œuvre.

Selon une caractéristique particulière, le procédé comporte une étape consistant à attribuer une durée de vie à chaque message en attente de réception par une entité électronique destinataire.

30 Cela permet de supprimer des messages dont le destinataire a disparu depuis longtemps. Selon les besoins de l'application, cette durée de vie, mise à une valeur spéciale (par exemple, 0), permet d'annuler des messages dès qu'on détecte que leur destinataire est hors de portée de l'unité de gestion des communications.

Selon une caractéristique particulière, le procédé comporte une étape consistant à affecter une priorité à chaque message échangé dans le cadre du protocole commande-réponse.

5 Cela permet au mécanisme de communication de traiter les messages prioritaires en premier.

Le procédé de communication conforme à la présente invention est adapté à la diffusion, par une des au moins deux entités électroniques, d'un message à destination de toutes les autres entités électroniques.

10 Cela permet par exemple de mettre en œuvre des mécanismes d'appel d'offre, par lesquels une entité désirant un service particulier émet un tel message de diffusion à destination de toutes les entités connues du système afin de recevoir une ou plusieurs propositions de réalisation de ce service.

Dans un mode particulier de réalisation, au moins une des entités électroniques est portable.

15 On peut ainsi tirer parti de tous les avantages pratiques de la portabilité.

Dans un mode particulier de réalisation, au moins une des entités électroniques communique avec l'unité de gestion des communications en utilisant une technologie sans contact.

20 Cela permet de nombreuses applications. L'entité électronique peut se passer de pile et de batterie et peut donc être réalisée sous une forme très compacte.

Dans un mode particulier de réalisation, au moins une des entités électroniques est sécurisée.

25 L'invention s'applique ainsi de façon privilégiée à la communication entre diverses entités électroniques sécurisées.

Au moins une des entités électroniques peut être une carte à microcircuit sans contact, telle qu'une carte bancaire sans contact, une carte de contrôle d'accès sans contact, ou une carte d'identité sans contact, à titre d'exemples non limitatifs.

30 De façon plus générale, au moins une des entités électroniques peut être une carte de fidélité, ou encore une carte de paiement.

Dans un mode particulier de réalisation, le procédé conforme à l'invention permet la continuité d'une communication impliquant une des entités

électroniques et une antenne parmi une pluralité d'antennes reliées à l'unité de gestion des communications lorsque cette entité électronique se déplace de façon que la communication précitée implique une autre antenne parmi la pluralité d'antennes mentionnée ci-dessus.

5 Dans une application privilégiée de la présente invention, les entités électroniques participent à un processus de personnalisation d'un objet sans contact et le processus comporte au moins une étape d'authentification mutuelle, réciproque ou non, entre les entités électroniques.

10 Cela permet notamment de vérifier que toutes les entités électroniques participant au processus de personnalisation sont habilitées à le faire.

Dans cette application, dans un mode particulier de réalisation, le processus de personnalisation comporte le passage de l'objet à personnaliser devant une pluralité de postes comportant chacun des moyens de communication sans fil et reliés à l'unité de gestion des communications, et le
15 procédé permet la continuité du processus de personnalisation lorsque l'objet passe d'un poste au suivant.

Toujours dans cette application, et dans ce mode de réalisation, l'objet peut communiquer avec la pluralité de postes précitée en utilisant une technologie sans contact.

20 Cette technologie est particulièrement adaptée aux documents de voyage et aux documents officiels, qui sont de plus en plus nombreux, dans leur version électronique, à mettre en œuvre cette technologie pour des raisons pratiques. On peut par exemple conserver le format d'origine d'un passeport et insérer dans le papier du passeport un microcircuit utilisant une technologie de
25 communication sans contact.

La présente invention permet de réaliser facilement et avec une grande robustesse une communication de type RMI ("Remote Method Invocation" de Java) entre les différentes entités électroniques du système.

30 D'autres aspects et avantages de l'invention apparaîtront à la lecture de la description détaillée qui suit de modes particuliers de réalisation, donnés à titre d'exemples non limitatifs. La description est faite en référence aux dessins qui l'accompagnent, dans lesquels :

- la figure 1 représente de façon schématique une unité de gestion des communications et diverses entités électroniques mettant en œuvre la présente invention ;

5 - la figure 2 est un organigramme illustrant les principales étapes effectuées lors de la mise en œuvre du procédé de communication conforme à la présente invention, dans un mode particulier de réalisation ;

10 - la figure 3 est un organigramme illustrant les principales étapes effectuées lors de l'arrivée d'une nouvelle entité électronique dans le rayon d'action de l'unité de gestion des communications conformément à l'invention, dans un mode particulier de réalisation ; et

- la figure 4 représente de façon schématique un dispositif de personnalisation d'objets mettant en œuvre la présente invention, dans un mode particulier de réalisation.

15 Comme le montre la **figure 1**, dans un mode particulier de réalisation, le procédé de communication conforme à la présente invention fait intervenir une unité de traitement logique (UTL) 10, qui remplit les fonctions d'une unité de gestion des communications utilisant un protocole de communication du type commande-réponse, et qui commande ainsi au moins en partie le déroulement des communications entre plusieurs entités électroniques 12₁, 12₂, 12₃.

20 Les entités électroniques 12₁ et 12₂ sont ici des cartes à microcircuit, sont chacune pourvues d'une antenne et communiquent avec l'UTL 10 en utilisant une technologie sans contact, tandis que l'entité électronique 12₃ est ici un SHM ou module de sécurité matériel (en anglais "*Secure Hardware Module*") et communique avec l'UTL 10 par l'intermédiaire d'une connexion filaire.

25 Cependant, de façon plus générale, les entités électroniques 12₁ et 12₂ peuvent communiquer avec l'UTL 10 en utilisant une technologie sans fil du type conforme à la norme Bluetooth, WiFi, etc. Le rayon d'action de l'UTL 10 est représenté en tirets sur le dessin et correspond ici à la région soumise à un champ radiofréquence.

30 Le procédé de communication conforme à la présente invention comporte une étape consistant à mémoriser dans l'UTL 10 une liste ("*liste*" sur le dessin) des entités électroniques qui sont en mesure de communiquer avec elle.

Les entités électroniques 12_1 , 12_2 et 12_3 forment un réseau d'acointances, c'est-à-dire qu'elles sont susceptibles d'échanger des messages.

Comme décrit en introduction, ce réseau d'acointances présente un caractère dynamique, c'est-à-dire qu'il évolue en fonction de l'arrivée d'une ou plusieurs nouvelles entités électroniques dans le rayon d'action de l'UTL 10 ou, inversement, lors de la sortie d'une ou plusieurs entités électroniques de ce rayon d'action.

Ainsi, lorsque l'entité électronique 12_4 , qui est ici une carte à microcircuit sans contact (mais qui pourrait aussi bien communiquer avec l'UTL en utilisant une technologie sans fil du type conforme à la norme Bluetooth, WiFi, etc.) entre en communication avec l'UTL 10, en arrivant dans son champ radiofréquence, cette entité est non seulement ajoutée dans la liste mémorisée dans l'UTL 10, mais en outre, la nouvelle entité 12_4 est enregistrée comme accointance de l'entité 12_1 si et seulement si ces deux entités sont amenées à communiquer entre elles par la suite et, de même, la nouvelle entité 12_4 est enregistrée comme accointance de l'entité 12_2 si et seulement si ces deux entités sont amenées à communiquer entre elles par la suite et la nouvelle entité 12_4 est enregistrée comme accointance de l'entité 12_3 si et seulement si ces deux entités sont amenées à communiquer entre elles par la suite. Pour déterminer ces accointances, on peut par exemple faire usage d'un critère C selon lequel deux entités du même type peuvent communiquer entre elles.

Par ailleurs, l'UTL 10 gère pour chacune des entités 12_1 , 12_2 et 12_3 présentes dans le système, une boîte aux lettres adaptée à mémoriser des messages en attente de traitement. Par exemple, si l'entité électronique 12_2 sort temporairement du champ radiofréquence et si l'UTL 10 reçoit un message qui est destiné à l'entité 12_2 , ce message est mémorisé dans la boîte aux lettres attribuée à l'entité 12_2 jusqu'à ce que l'entité 12_2 revienne dans le champ radiofréquence. De même, si l'entité 12_3 se déconnecte temporairement de l'UTL 10 et si l'UTL 10 reçoit un message destiné à l'entité 12_3 , ce message est mémorisé dans la boîte aux lettres attribuée à l'entité 12_3 jusqu'à ce que l'entité 12_3 se connecte à nouveau à l'UTL 10.

Lorsque la nouvelle entité 12₄ entre dans le réseau, une boîte aux lettres est créée dans l'UTL pour cette entité et comporte les messages en attente de traitement par la nouvelle entité 12₄.

Si une entité électronique sort du champ radiofréquence ou est
5 déconnectée physiquement de l'UTL 10 et si sa boîte aux lettres est vide et qu'aucune de ses accointances n'a de message qui lui soit destiné, alors cette entité est supprimée du réseau.

Chaque entité électronique est repérée par un identifiant unique. Typiquement, on choisit l'identifiant décrit dans la norme ISO 14443 part 3 ou la
10 norme ISO 7816-6/AM1. A cet identifiant est avantageusement associé un code de service ou de famille décrivant les possibilités supportées par l'entité et participant au critère d'accointance C entre entités.

Ainsi, lorsque l'entité 12₁ veut envoyer un message à l'entité 12₂, elle peut le faire en indiquant l'identifiant de l'entité 12₂ ou en précisant uniquement le
15 code de service ou de famille de l'entité 12₂. Dans ce cas, l'UTL 10 choisit toujours le même destinataire d'un message sur l'autre pour un code de service ou de famille identique. En variante et selon la nature de l'application, on peut utiliser toute méthode, déterministe ou non, pour choisir le destinataire d'un message par son code de service ou de famille.

20 L'organigramme de la **figure 2** illustre les principales étapes effectuées par l'UTL 10 lors de la mise en œuvre d'un procédé de communication conforme à l'invention.

L'UTL 10 parcourt la liste des entités électroniques. Pour chaque entité E du réseau (étape E80), l'UTL 10 examine si la boîte aux lettres B attribuée à E
25 est vide ou non (test E82). Si B est vide, l'UTL 10 envoie un message d'interrogation à E (étape E84). L'UTL 10 vérifie ensuite si E renvoie ou non un accusé de réception (test E86). Si E renvoie un accusé de réception, l'UTL 10 effectue le même échange avec l'entité électronique suivante (étapes E82, E84, E86).

30 Sinon, c'est-à-dire si E ne renvoie pas d'accusé de réception, l'UTL 10 vérifie si l'entité E répond qu'elle a un message M à envoyer à une entité D ou non (test E88). Si E a un message M pour D, l'UTL 10 place M dans la boîte aux

lettres de D, puis le processus reprend pour l'entité électronique suivante à partir du test E82.

Si, lors du test E88, E ne répond plus, l'UTL 10 supprime E du réseau, puis le processus reprend pour l'entité électronique suivante à partir du test E82.

5 Si, lors du test E82, la boîte aux lettres B de E n'est pas vide, l'UTL 10 envoie à E le message M le plus ancien de B (étape E94). Ensuite, l'UTL 10 vérifie si E renvoie un accusé de réception du message M (test E96). Si ce n'est pas le cas, le processus reprend pour l'entité électronique suivante à partir du test E82. Sinon, c'est-à-dire si E accuse réception du message M, l'UTL 10
10 supprime M de B (étape E98). Dans le cas le plus courant, B est une boîte de réception. Cependant, en variante, B pourrait aussi bien être une boîte d'émission.

L'organigramme de la **figure 3** rappelle le mécanisme mis en œuvre lors de l'arrivée (étape E30) d'une nouvelle entité électronique dans le rayon d'action
15 de l'UTL 10. L'UTL 10 crée une boîte aux lettres B pour E (étape E32) puis vérifie si le critère C déterminant l'ajout de E dans le réseau d'acointances est satisfait ou non (test E34). Si c'est le cas, l'UTL 10 ajoute E au réseau d'acointances (étape E36) et, pour chaque entité déjà présente dans le réseau, enregistre E comme accointance de cette ancienne entité si et seulement si les
20 deux entités sont amenées à communiquer entre elles par la suite.

Le réseau d'acointances peut être réalisé de diverses façons. Dans la mémoire de l'UTL 10, il peut par exemple prendre la forme d'une table d'acointances dynamiques, c'est-à-dire une table de correspondance associant,
à chaque entité électronique, ses accointances. En variante, le réseau
25 d'acointances peut être réparti dans la mémoire de chacune des entités électroniques, chacune d'entre elles ayant alors connaissance de ses propres accointances.

Diverses variantes et améliorations au mode de réalisation décrit précédemment peuvent être envisagées.

30 L'UTL peut être vue comme une entité électronique toujours connectée au système. Elle possède alors son propre identifiant, son code de service ou de famille et sa boîte aux lettres pour recevoir des messages en provenance des autres entités électroniques. On parle d'UTL participante.

Une des entités électroniques peut être accessible indirectement par un système d'indirection ou proxy au travers d'un réseau ouvert quelconque. L'UTL peut alors servir de proxy à cette entité lointaine.

On peut prévoir une information temporelle TTL (en anglais "*Time To Live*") qui détermine la durée de vie d'un message en attente de présence de son destinataire. Ce mécanisme permet de supprimer des messages devenus obsolètes en raison de la disparition de leur destinataire depuis longtemps. Dans certaines applications, le paramètre TTL, mis à une valeur spéciale (par exemple, la valeur 0), peut aussi permettre d'annuler un message dès qu'on détecte que son destinataire est hors de portée de l'UTL.

Une priorité P peut être affectée aux messages. Dans ce cas, le mécanisme de communication fera passer les messages les plus prioritaires en premier.

Selon l'application envisagée, il peut être avantageux d'utiliser un mécanisme d'appel d'offre : une entité qui souhaite un service particulier émet à cet effet un message de diffusion ou "broadcast" à destination de toutes les entités électroniques connues du système, c'est-à-dire à tous les éléments de la liste mémorisée dans l'UTL. La ou les entités intéressées peuvent émettre une proposition de réalisation du service que l'entité demanderesse peut accepter ou refuser selon des critères qui lui sont propres.

L'ensemble du mécanisme d'appel d'offre (le message "broadcast", les réponses puis le message d'acceptation par l'entité demanderesse) utilise le procédé de communication de l'invention. A l'issue de l'appel d'offre, l'UTL peut compléter sa table d'acointances dynamiques, par exemple en indiquant que telle ou telle entité sait ou ne sait pas réaliser tel service.

On peut associer un paramètre TTL au message "broadcast".

Lors de l'entrée d'une nouvelle entité dans le rayon d'action de l'UTL, un message "broadcast" particulier est diffusé à l'ensemble des entités déjà présentes dans le réseau. Ce message indique notamment l'identifiant de l'entrant ainsi que son code de service ou de famille. Ce mécanisme est appelé "Diffusion sur entrant".

De façon analogue, lors de la sortie d'une entité électronique du rayon d'action de l'UTL, un message "broadcast" particulier est diffusé à l'ensemble

des entités encore présentes dans le réseau. Ce message indique notamment l'identifiant du sortant ainsi que son code de service ou de famille. Ce mécanisme est appelé "Diffusion sur sortant".

5 Lorsque plusieurs entités électroniques participent à un calcul distribué, il est possible de voir l'envoi d'un message M1 d'une entité E1 vers une entité E2 comme une demande de calcul. Dans ce message, une entité E3 de continuation explicite du calcul peut être précisée. Ainsi, lorsque l'entité E2 aura terminé le calcul effectué lors de la réception des éléments du message M1, elle enverra la demande de continuation de calcul en envoyant un message M2 à
10 l'entité E3.

On donne maintenant divers exemples d'utilisation de l'invention.

Tout d'abord, dans le domaine de la fidélisation des clients dans le transport aérien, on considère un voyageur qui possède une carte de fidélité de la compagnie aérienne X. Le voyageur achète un billet de transport de la
15 compagnie X et se présente au salon VIP pour patienter avant l'embarquement.

Une hôtesse est munie d'un terminal de localisation supposé de nouvelle génération, capable d'utiliser le mécanisme de la présente invention. Elle possède une carte hôtesse munie d'une application de gestion de la clientèle.

Lorsque le voyageur passe à proximité du terminal de l'hôtesse, sa carte
20 de fidélité et son billet de transport se déclarent à ce terminal. La carte hôtesse, après authentification adéquate, demande au billet de transport l'identifiant du voyageur et demande à la carte de fidélité le nombre de points de fidélité associés à ce voyageur.

Si la carte hôtesse détecte un client fidèle (ayant un nombre de points de
25 fidélité dépassant un certain seuil), l'hôtesse offre par exemple au voyageur sa boisson préférée, information mémorisée dans la carte de fidélité. Puis la carte hôtesse transfère à la carte de fidélité par exemple un bon d'achat valable dans une des boutiques de la zone franche.

A titre de deuxième exemple, on considère un client possédant dans son
30 portefeuille une carte bancaire et une carte de fidélité. En plus de leur mode de fonctionnement classique, les deux cartes savent communiquer de façon sécurisée par l'intermédiaire d'une interface sans contact.

On considère également un commerçant possédant un terminal de paiement de nouvelle génération, capable d'utiliser le mécanisme de la présente invention.

Le client effectue un paiement avec sa carte bancaire en saisissant son code confidentiel de façon classique, mais en ne sortant pas sa carte bancaire de son portefeuille. Une fois le paiement validé, la carte bancaire envoie un message "broadcast" à la recherche d'un service de fidélité pour le magasin où l'achat vient d'être effectué. La carte de fidélité propose ses services en précisant qu'elle accepte de mémoriser des points de fidélité conformément à la demande de la carte bancaire.

La carte bancaire transmet alors à la carte de fidélité le nombre de points de fidélité à créditer au compte du client et la carte de fidélité crédite ces points.

Au cas où une autre carte de fidélité, telle que la carte d'un opérateur de transport, est présente dans le portefeuille de ce client, cette autre carte peut aussi demander à la carte bancaire la nature de l'achat avant de proposer ses services. Une communication entre les trois entités électroniques est alors entreprise.

Afin de sécuriser les échanges entre ces diverses entités, une quatrième entité électronique peut être insérée dans le corps du terminal de paiement (entité électronique sécurisée du type SHM), qui participe à certaines authentifications pour le compte des trois autres entités électroniques.

On décrit maintenant un exemple d'application de l'invention à la personnalisation d'objets. Par personnalisation, on entend l'écriture, dans ou sur l'objet, par voie mécanique, électronique, optique, chimique ou par toute autre technique, de données personnelles propres à cet objet.

On considère une machine de personnalisation comportant plusieurs postes. L'objet à personnaliser se trouve placé pendant une durée déterminée devant chaque poste puis est déplacé vers le poste suivant. Le passage d'un poste à un autre n'étant pas défini de façon rigoureuse au plan temporel, certains messages risquent d'être perdus lors du passage d'un poste au suivant.

La figure 4 illustre un tel dispositif. Une UTL 40 est connectée à un module de sécurité matériel SHM 42 et à trois antennes a1, a2, a3 désignées par le chiffre de référence 46. Les antennes 46 correspondent chacune à un

poste de travail d'une machine à personnaliser des objets 44 qui se déplacent de poste en poste. Le SHM 42 contient les informations nécessaires à la personnalisation. La flèche 48 sur le dessin délimite une "zone d'ombre" ou de perturbations radiofréquences dans laquelle passe l'objet à personnaliser entre deux postes de travail successifs.

L'invention s'applique ici avantageusement aux entités électroniques constituées par le SHM 42 et l'objet à personnaliser 44. Ainsi, l'objet disparaît de la liste des accointances dynamiques lorsqu'il entre dans la zone 48 puis réapparaît dans celle-ci lorsqu'il se présente devant un nouveau poste de travail.

Lorsque l'objet est dans la zone 48, les messages en cours sont sauvegardés dans des boîtes aux lettres conformément à l'invention, comme décrit plus haut. Ainsi, il y a continuité de la communication entre l'objet 44 et le SHM 42 via l'UTL 40 et les diverses antennes 46.

Plus généralement, le procédé selon l'invention permet la continuité d'une communication impliquant une entité électronique et une antenne parmi une pluralité d'antennes reliées à une unité de gestion des communications lorsque cette entité électronique se déplace de façon que la communication implique une autre antenne parmi la pluralité d'antennes précitée.

Enfin, la présente invention peut avantageusement être utilisée pour la personnalisation sécurisée d'un objet comportant un premier ensemble sécurisé constitué d'une première unité de mémorisation et d'un premier microcircuit, dans un procédé de personnalisation qui met en œuvre $n-1$ ensembles sécurisés en plus du premier ensemble sécurisé, n étant un entier strictement supérieur à 2, chacun de ces ensembles sécurisés étant constitué d'une unité de mémorisation et d'un microcircuit, et formant avec l'objet un n -uplet autorisé, connu d'au moins un des ensembles sécurisés, le procédé de personnalisation comportant une pluralité d'étapes d'authentification entre les ensembles sécurisés pris deux à deux, préalablement à une étape de personnalisation consistant à écrire, dans ou sur l'objet, des données personnelles propres à cet objet.

Un ou plusieurs des microcircuits précités peuvent être adaptés à communiquer avec l'extérieur en utilisant une technologie sans contact.

L'objet à personnaliser est par exemple un titre émis par l'Etat, tel qu'une carte d'identité, un passeport, un visa ou une carte grise (en anglais "*vehicle registration papers*"), ou un autre document à caractère officiel, tel qu'un acte notarié, ou encore un titre de transport, tel qu'une carte d'abonnement pour emprunter les transports en commun, ou un document de voyage, tel qu'un permis de conduire, ou un ticket de péage ou autre justificatif d'un droit à transiter, du type des autorisations délivrées par exemple par la ville de Mexico aux automobilistes, pour entrer dans la ville.

Les n-1 ensembles sécurisés mentionnés ci-dessus peuvent être pris parmi :

- un ensemble sécurisé représentant un lot d'objets à personnaliser,
- un ensemble sécurisé comportant une entité électronique sécurisée associée à une machine adaptée à personnaliser les objets de ce lot, et
- un ensemble sécurisé attaché à un opérateur habilité à utiliser cette machine.

Cela permet de personnaliser de façon sécurisée tout objet faisant partie d'un lot, tel qu'une carte d'identité prise parmi un lot initial de cartes à personnaliser, la personnalisation étant effectuée au moyen d'une machine habilitée identifiée par un module sécurisé machine associé, et où la machine est manipulée par un opérateur habilité identifié par exemple par une carte à microcircuit opérateur en sa possession, qui l'identifie de façon unique.

Pour plus de détails sur ce procédé de personnalisation, on se reportera à la demande de brevet français n° 02 15551.

REVENDICATIONS

1. Procédé de communication entre au moins deux entités électroniques (12₁, 12₂, 12₃), ledit procédé faisant intervenir des moyens (10) de gestion des communications qui utilisent un protocole commande-réponse pour communiquer avec lesdites entités électroniques (12₁, 12₂, 12₃), ledit procédé étant caractérisé en ce qu'au moins une desdites entités électroniques (12₁, 12₂) communique avec lesdits moyens (10) de gestion des communications en utilisant une technologie sans fil, et en ce qu'il comporte une étape consistant à mémoriser dans les moyens (10) de gestion des communications une liste desdites entités électroniques.

2. Procédé selon la revendication 1, caractérisé en ce que lesdites entités électroniques (12₁, 12₂, 12₃) forment un réseau d'accointances.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce qu'il comporte une étape consistant à mémoriser un message destiné à au moins une desdites au moins deux entités électroniques (12₁, 12₂, 12₃) lorsque l'entité électronique destinataire est temporairement hors de portée des moyens (10) de gestion des communications.

4. Procédé selon la revendication 1, 2 ou 3, caractérisé en ce qu'à chacune desdites au moins deux entités électroniques (12₁, 12₂, 12₃) est associé un identifiant unique.

5. Procédé selon la revendication précédente, caractérisé en ce qu'à chaque identifiant est associé un code de service ou de famille.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte une étape consistant à créer une boîte aux lettres dans les moyens (10) de gestion des communications lorsque ladite liste comporte une nouvelle entité électronique, ladite boîte aux lettres étant adaptée à recevoir et mémoriser des messages destinés à ou envoyés par ladite nouvelle entité électronique.

7. Procédé selon la revendication 2, caractérisé en ce qu'il comporte une étape consistant, lorsque ladite liste comporte une nouvelle entité électronique, à ajouter la nouvelle entité électronique audit réseau d'accointances en fonction d'au moins un critère prédéterminé.

8. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte des étapes suivant lesquelles lesdits moyens (10) de gestion des communications :

- parcourent (E80) ladite liste des entités électroniques,
- 5 - demandent (E84) à chaque entité électronique si elle a un message à envoyer et, si c'est le cas,
- mémorisent (E90) ledit message dans une boîte aux lettres,
- envoient (E94) ledit message à l'entité électronique destinataire du message lorsqu'elle est joignable, puis
- 10 - suppriment (E98) le message de ladite boîte aux lettres.

9. Procédé selon la revendication précédente, caractérisé en ce que ladite boîte aux lettres est une boîte de réception.

10. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il fait intervenir au moins trois entités électroniques et en ce que lesdits moyens (10) de gestion des communications se confondent avec une desdites entités électroniques.

11. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdits moyens (10) de gestion des communications servent de proxy pour accéder à au moins une desdites au moins deux entités électroniques.

12. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte une étape consistant à attribuer une durée de vie (TTL) à chaque message en attente de réception par une entité électronique destinataire.

13. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comporte une étape consistant à affecter une priorité (P) à chaque message échangé dans le cadre dudit protocole commande-réponse.

14. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il est adapté à la diffusion, par une desdites au moins deux entités électroniques, d'un message (BROADCAST) à destination de toutes les autres entités électroniques.

15. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'au moins une desdites au moins deux entités électroniques est portable.

5 16. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'au moins une desdites au moins deux entités électroniques communique avec les moyens (10) de gestion des communications en utilisant une technologie sans contact.

10 17. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'au moins une desdites au moins deux entités électroniques est sécurisée.

18. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'au moins une desdites au moins deux entités électroniques est une carte à microcircuit sans contact.

15 19. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'au moins une desdites entités électroniques est une carte de fidélité.

20. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'au moins une desdites entités électroniques est une carte de paiement.

20 21. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il permet la continuité d'une communication impliquant une desdites entités électroniques et une antenne parmi une pluralité d'antennes reliés aux moyens de gestion des communications lorsque ladite entité électronique se déplace de façon que ladite communication implique une autre
25 antenne parmi ladite pluralité d'antennes.

22. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que lesdites entités électroniques participent à un processus de personnalisation d'un objet sans contact et en ce que ledit processus comporte au moins une étape d'authentification mutuelle, réciproque ou non,
30 entre les entités électroniques.

23. Procédé selon la revendication précédente, caractérisé en ce que ledit processus comporte le passage de l'objet à personnaliser (44) devant une pluralité de postes (46) comportant chacun des moyens de communication sans

fil et reliés aux moyens (10) de gestion des communications, et en ce que ledit procédé permet la continuité du processus de personnalisation lorsque l'objet passe d'un poste au suivant.

- 5 24. Procédé selon la revendication précédente, caractérisé en ce que l'objet communique avec ladite pluralité de postes en utilisant une technologie sans contact.

1/3

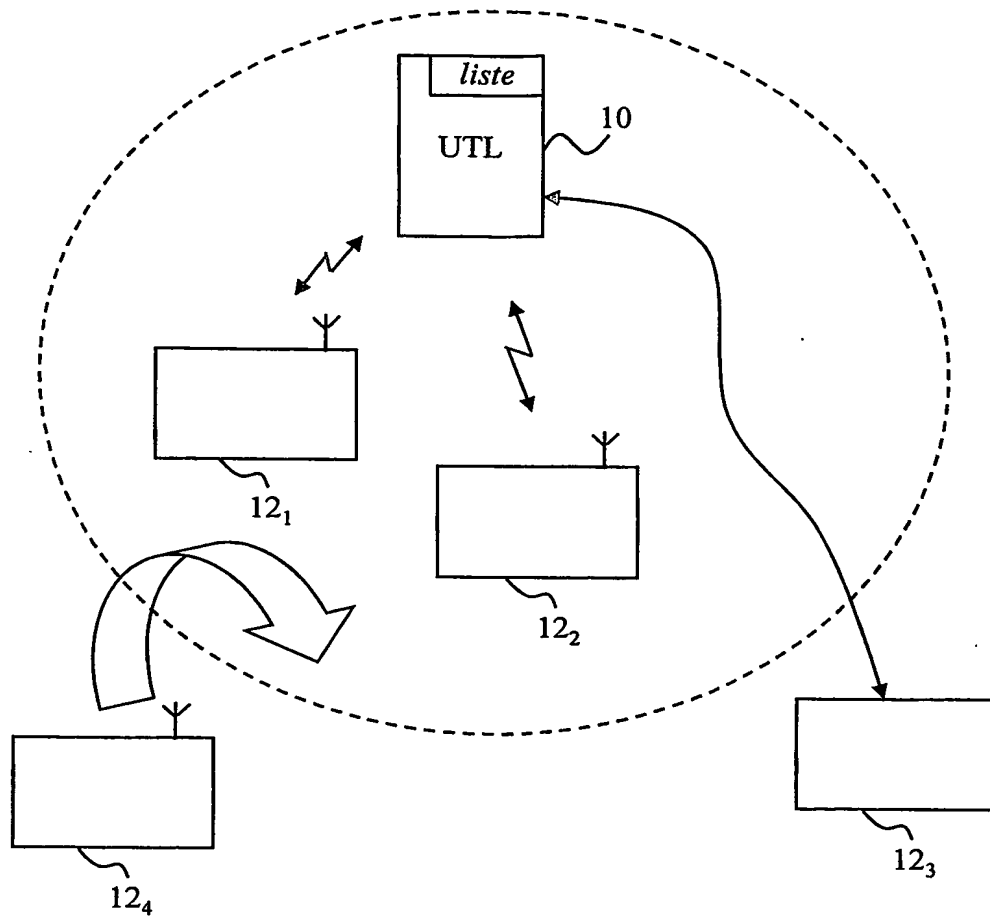


FIG. 1

2/3

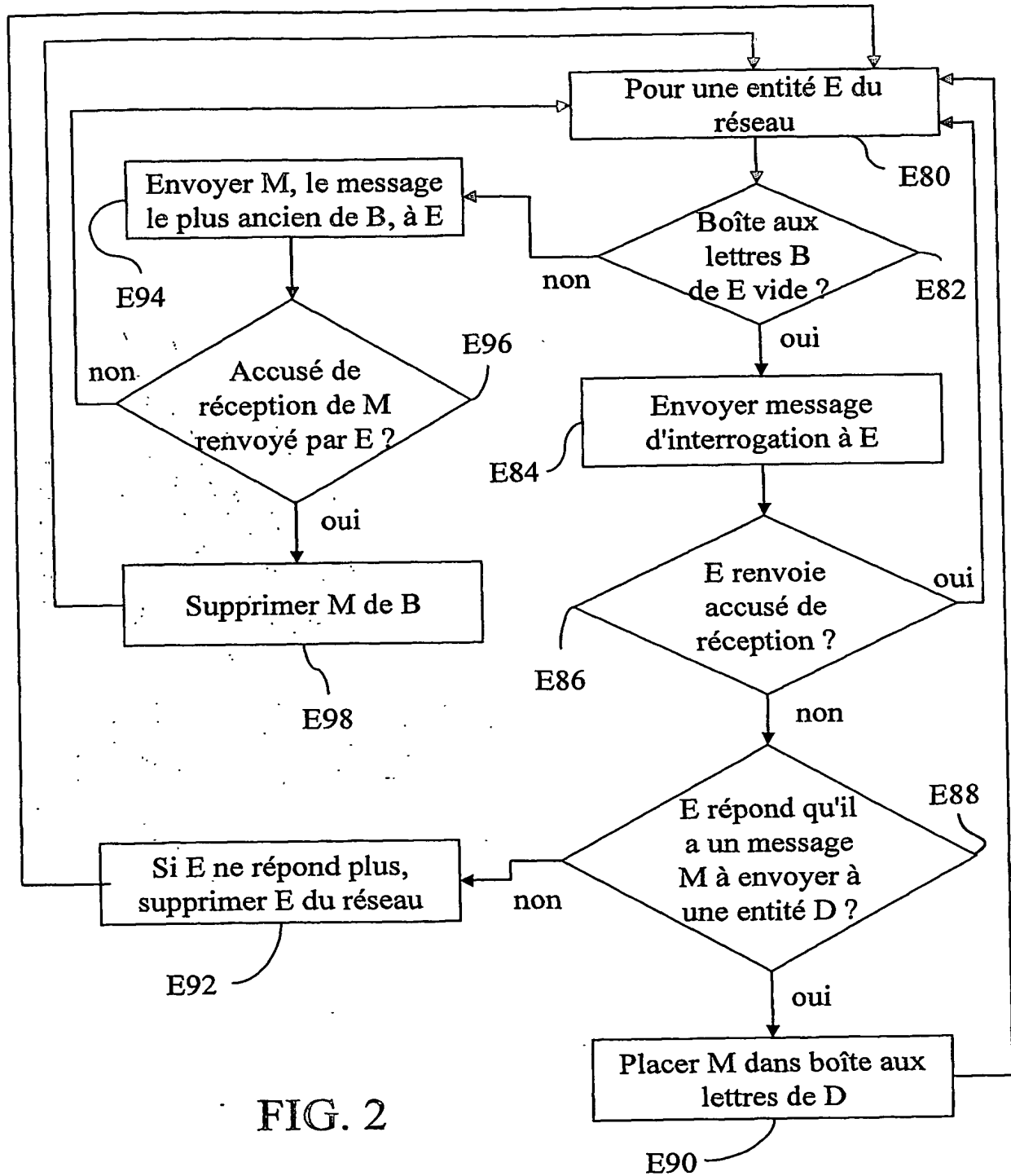


FIG. 2

3/3

FIG. 3

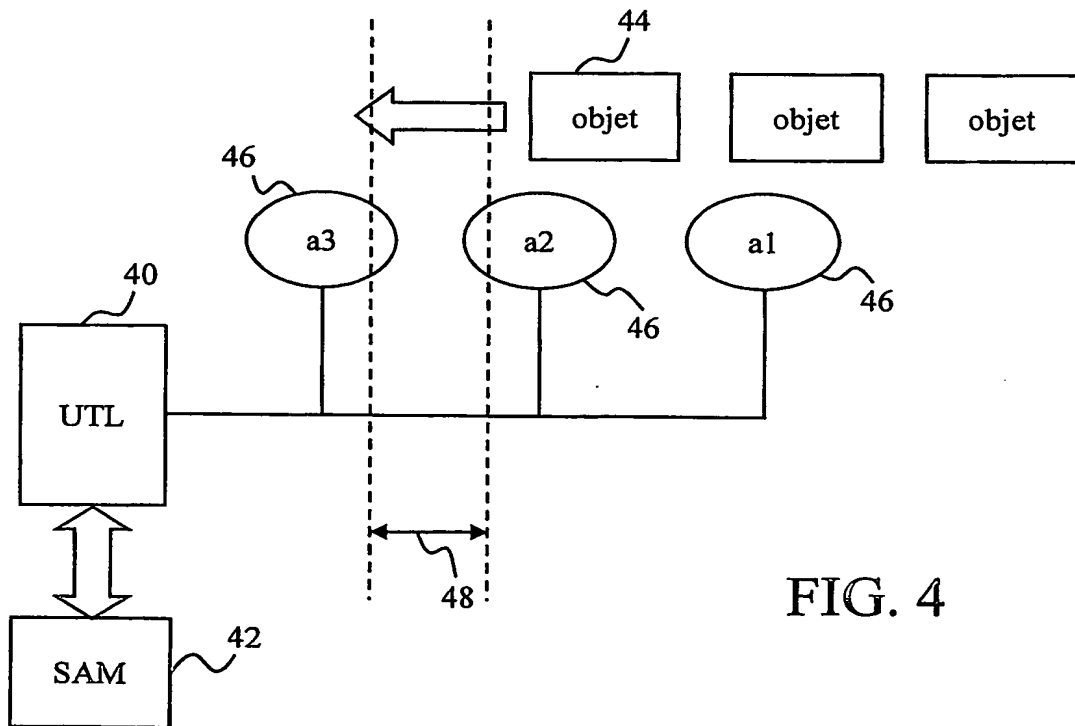
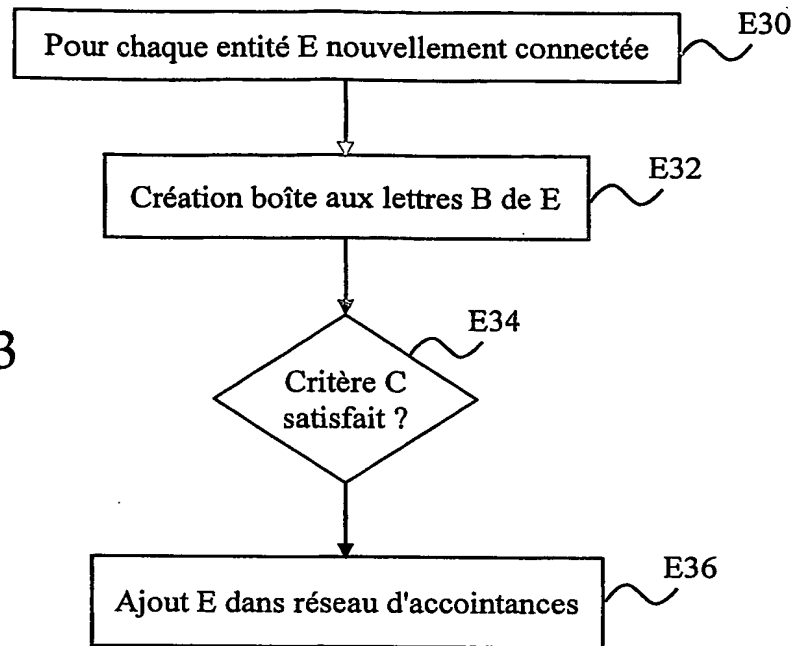


FIG. 4